IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI SOUTHERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 13-03081-01-CR-S-MDH
	)	
MARK RICHARD DALLMAN,	)	
	)	
Defendant.	)	

REPORT & RECOMMENDATION OF U.S. MAGISTRATE JUDGE

Pursuant to 28 U.S.C. § 636(b), the above-styled criminal action was referred to the undersigned for preliminary review. Defendant moves to suppress evidence and statements obtained from the search of his computer on September 5 and 12, 2013. (Doc. 76.) He argues that the search violated his Fourth Amendment rights because Deputy United States Marshal Michael Walker exceeded the scope of the search warrant obtained to search his computer. (*Id.*) The Government argues Deputy Walker searched the computer pursuant to two valid search warrants and that his actions are supported by case law. (Doc. 78.) On August 4, 2016, the undersigned held a hearing on the Motion. (*See* Doc. 88.) Defendant was present with his attorney, Kristin Jones, and the Government was represented by Assistant United States Attorney Patrick Carney. (*See id.*) During the hearing, the Court received evidence and heard testimony from Deputy United States Marshal Michael Walker; Detective Larry Roller of the Joplin, Missouri Police Department; and Tami Loehrs, a computer and forensics expert. After careful review of the evidence and for the reasons set forth below, it is hereby **RECOMMENDED** that Defendant's Motion, (Doc. 76), be **GRANTED** and that the evidence obtained as a result of the search of Defendant's computer on September 5, 2013 be **SUPPRESSED**.

I. Findings of Fact[1]

On August 22, 2013, Deputy Walker was notified that Defendant had been arrested by the Howell County Sheriff's Office. Defendant had allegedly been living in Missouri for over one year under the assumed name John Sanders. A records check determined that Defendant was a convicted sex offender and had not registered as required by law. On August 23, 2013, Deputy Walker went to West Plains, Missouri to interview Defendant and collect various forms of identification with the name John Sanders. Defendant was read his *Miranda* rights and subsequently admitted to obtaining a false identity through the internet.

On September 5, 2013, Deputy Walker obtained a search warrant to search for evidence relevant to the identity theft and the failure to register as a sex offender. His affidavit supporting the search warrant stated that he believed evidence of those crimes would be on Defendant's computer, as well as evidence of Defendant's travel between May 2007 and August 23, 2013. In relevant part, that warrant provided the following items would be searched and seized:

1. All documents, records, materials, and items related to telephone bills/toll documents;

2. All documents, records, materials, and items related to travel records (including indicia of airline expenses, lodging receipts, car rentals, and other travel related expenses);

3. All documents, records, materials, and items related to charge card records;

4. All documents, records, materials, and items, in any electronic format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online

[1] The facts set forth herein are taken from the testimony adduced and the exhibits admitted at the hearing on the instant Motion. The hearing transcript appears as Doc. 88. The Government's exhibit index appears as Doc. 86, and Defendant's exhibit index appears as Doc. 87.

storage or remote computer storage related to any and all documents described above in items 1-3;

5. All documents, records, materials, and items related to electronic records of websites visited relating to travel, and residency;

6. All documents, records, materials, and items related to indicia of use and/or residency at 3731 South Glenstone, Lot 505, Springfield, Missouri, 11020 East State Highway 76, Forsyth Missouri, 18412 North Old highway 65, Omaha, Arkansas, or 4678 West Highway 160, West Plains, Missouri.

7. All documents, records, materials, and items related to electronic records, receipts, notes, correspondence, electronic mail, short message service messages, multi-media message service messages, weblogs, microblogs (i.e., Twitter, Identica, etc.), social websites (i.e., Facebook, My Space, etc.), ledgers, related to travel and residency; and,

8. All documents, records, materials, and items related to passwords, encryption keys, and other access devices that may be necessary to access the computer.

(Gov. Ex. 1.) The warrant did include the search and seizure of evidence of child pornography, and no such permission was sought to search and seize such evidence.

On September 6, 2013, Deputy Walker arrived at Defendant's residence with other officers to execute the warrant. He began the search when he inserted a thumb drive containing a software search program known as OS Triage into Defendant's computer. The program is provided by the FBI for investigations of electronics, particularly for use in examining or previewing a Windows operating system. It also allows an individual to search the contents of a computer using keywords. Additionally, the program has or utilizes a database of known images of child pornography and can conduct automatic keyword searches related to known images of child pornography. In this case, the program automatically conducted a search for known images of child pornography by using both the database and keyword search, and Deputy Walker knew it would. Deputy Walker has received some training to use this software program. He testified that OS Triage is used in almost all cases involving FBI searches of computers that use Windows

operating systems, including fraud cases, threat cases, stalking or harassment cases, and child pornography cases.

When Deputy Walker plugged the thumb drive, it began to run an analysis of Defendant's computer. While the program was running, Deputy Walker and the other officers began a physical search of Defendant's residence. About an hour after initiating the computer search and starting the physical search, Deputy Walker turned his attention back to Defendant's computer. He saw that the computer was displaying an image outlined with a red boarder on the screen. Based on his training and knowledge, Deputy Walker knew that this display meant that OS Triage had located a file containing child pornography.[2] He had not done any individualized keyword searches or done anything other than plug the thumb drive into the computer. However, he did not know long OS Triage continued to search the computer after it located the one image of child pornography. At that point, Deputy Walker instructed the software to shut down and disconnected the computer. He then seized the computer as evidence and contacted the United States Attorney's Office, which advised him to obtain a second search warrant before examining the computer further. A log of the OS Triage search indicates there were a total of 41,753 files searched, including 480 videos and 36,426 images, before Deputy Walker shut down the program.

Deputy Walker received a second search warrant on September 12, 2013. In his affidavit, Deputy Walker provided the information about the previous search of Defendant's computer and discovering the thumbnail image of child pornography. This second warrant sought to search Defendant's computer again, expanding the search for evidence of receipt and possession of child pornography. The computer remained in the custody of law enforcement as of the time Deputy Walker seized it on September 6, 2013. Deputy Walker contacted Larry

[2] The specific file located by the program was a video file containing known child pornography.

Roller, a detective with the Joplin, Missouri Police Department and a Task Force Officer with the Southwest Missouri Cyber Crimes Task Force, to help him with the forensic examination pursuant to the second search. Det. Roller has several years of experience with forensic examinations of computers, taken numerous training courses, and received certification in certain forensic examination programs. He is familiar with the operation of OS Triage and has used it many times in the field and in his lab. Det. Roller affirmed that OS Triage is used in a number of different kinds of cases, including fraud cases. He also confirmed that OS Triage's standard settings would automatically search for child pornography (among other things), as it did during the search of Defendant's computer, even if a search warrant did not allow it.

In late 2013, Det. Roller conducted a forensic examination of Defendant's computers, DVDs, and CDs. Det. Roller located only the one video containing child pornography on Defendant's computer. In 2015, Det. Roller conducted an examination of a mirror image of Defendant's computer using a more sophisticated software that allowed him to observe what searches Defendant conducted on his computer. That search revealed that Defendant had searched for and viewed other images and videos containing child pornography.

During the hearing, the Court also heard testimony from Tami Loehrs, a computer forensics expert. Ms. Loehrs has a number of different forensic certifications and holds a private investigator agency license. She also owns a computer forensics company in Tucson, Arizona. She has conducted over 700 forensic computer examinations since 1999, and has worked on a variety of civil and criminal cases. In her experience, she has only seen OS Triage used in cases where law enforcement search specifically for child pornography. Though Ms. Loehrs was not able to examine OS Triage because it a proprietary law enforcement tool, she has used several publicly available software programs that operate in a similar way. She offered the opinion that,

had she been doing a search tailored to residency and travel on a computer using a software program like OS Triage, it would be unlikely that she would come across the video containing child pornography.

II. Conclusions of Law

Defendant argues that the Government exceeded the scope of the first warrant in violation of his Fourth Amendment rights. Specifically, he contends that Deputy Walker used OS Triage knowing that it would specifically search for child pornography, among other things, which was outside the scope of the search for evidence of the failure to register as a sex offender and identity theft. He thus contends that any evidence discovered as a result of the illegal search should be suppressed. The Government makes three arguments to support the position that the evidence was legally obtained. First, it contends that Deputy Walker proceeded in the appropriate manner by stopping the search as soon as the child pornography was discovered and obtaining a second warrant. Second, the Government argues that the search did not exceed the scope of the warrant because officers were authorized to search all the data on Defendant's computer for evidence of failure to register as a sex offender and identity theft; thus, the officers would have found the video when searching all the data. Third, it contends that the search by Det. Roller in 2015 showing that Defendant searched for and viewed child pornography was lawful. The Court takes up the parties' arguments below.

The Fourth Amendment requires search warrants be based on probable cause, supported by oath, and describe particularly the place to be searched and items to be seized. U.S. Const. amend. IV.; *United States v. Thomas*, 263 F.3d 805, 807 (8th Cir. 2001). "The general touchstone of reasonableness which governs Fourth Amendment analysis . . . governs the method of execution of the warrant." *United States v. Ramirez*, 523 U.S. 65 (1998) (internal citation

omitted); *see also United States v. Weinbender*, 109 F.3d 1327, 1329 (8th Cir. 1997) ("[t]he manner in which a warrant is executed is always subject to judicial review to ensure that it does not traverse the general Fourth Amendment proscription against unreasonableness.") (quotation omitted). "If the scope of the search exceeds that permitted by the terms of a validly issued warrant," then any derivative seizure or search should be suppressed as "fruit of the poisonous tree." *Horton v. California*, 496 U.S. 128, 140 (1990); *United States v. McManaman*, 673 F.3d 841, 846 (8th Cir. 2012). Officials executing a search warrant "must ensure that the search is conducted in a way that minimizes unwarranted intrusions into an individual's privacy." *United States v. Gregoire*, 2009 WL 5216844, at *8 (D. Minn. Dec. 29, 2009), aff'd, 638 F.3d 962 (8th Cir. 2011) (citing *United States v. Sparks*, 265 F.3d 825, 831 (9th Cir. 2005), overruled on other grounds by *United States v. Grisel*, 488 F.3d 844 (9th Cir. 2007)). Thus, searching anything but those items and areas specified in the warrant exceeds the scope of the warrant. *See United States v. Longie*, 370 F. Supp. 2d 941, 944 (N.D. Jan. 31, 2005). Though it is initially the defendant's burden to produce some evidence to show that a hearing is required to address a motion to suppress, it is the government's "ultimate burden of persuasion to show that its evidence is untainted" once an illegal search has come to light. *United States v. Williams*, 690 F. Supp. 2d 829 (D. Minn. 2010) (quoting *Alderman v. United States*, 394 U.S. 165, 183 (1969); *Carter v. United States*, 729 F.2d 935, 940 (8th Cir. 1984)).

The Government's argument about Deputy Walker following the appropriate procedure in obtaining a second warrant after discovering child pornography is misplaced. In each of those cases, officers either had unrestricted consent to search a computer and found images of child pornography, or happened upon child pornography while searching within the parameters of a valid search warrant. *United States v. Suing*, 712 F.3d 1209, 1211 (8th Cir. 2013) (in an

investigation for drug activity, defendant gave unlimited consent to search his computer and officers found thousands of images and videos containing child pornography); *United States v. Koch*, 625 F.3d 470, 476 (8th Cir. 2010) (agents were reviewing evidence pursuant to a judicial disposal order to see if it contained gambling information when they encountered child pornography on a thumb drive that was seized under a valid search warrant); *United States v. Hudspeth*, 459 F.3d 922, 928 (8th Cir. 2006), *opinion reinstated in part on reh'g en banc*, 518 F.3d 954 (8th Cir. 2008) (agent was reviewing CDs for evidence of drug activity pursuant to a search warrant, and found child pornography). Those officers then immediately stopped their searches to obtain a second warrant for child pornography. *Suing*, 712 F.3d at 1212 (upon discovering child pornography, the officer "immediately stopped the search, called a prosecutor for advice, and obtained a new warrant authorizing the search for child pornography."); *Koch*, 625 F.3d at 476; *Hudspeth*, 459 F.3d at 928. The Eighth Circuit determined that none of those searches exceeded the scope of the warrant or consent. *Suing*, 712 F.3d at 1212 ("the officer did not exceed the scope of [defendant's] consent, even assuming the consent was limited to a search of the vehicle for evidence of drug activity."); *Koch*, 625 F.3d 470, 476 (search of thumb drive did not exceed the scope of the warrant because agents were looking for evidence of gambling when they discovered child pornography); *Hudspeth*, 459 F.3d at 928.

In this case, the search exceeded the scope of the warrant from the beginning. Though the language of the warrant allowed officers to search through the data on Defendant's computer, *see Hudspeth*, 459 F.3d at 927-28 (concluding that a search warrant allowing for the search of "any and all" records included records on the computer), the search was specifically limited to items related to Defendant's travel, residency, and identity. (*See* Gov. Ex. 1.) Each witness at the hearing testified that OS Triage has standard settings that automatically search a computer for

images containing child pornography, through both an automatic keyword search and utilization of the FBI's database of known images of child pornography. Deputy Walker testified that he knew that the program worked in this way when he ran OS Triage on Defendant's computer. As such, Deputy Walker had knowledge that OS Triage would search for items that were outside the parameters of the warrant.[3] *Koch*, 625 F.3d at 477 ("Evidence should be suppressed 'only if it can be said that the law enforcement officer[s] had knowledge, or may be properly charged with knowledge, that the search was unconstitutional under the Fourth Amendment.'") (quoting *Illinois v. Krull*, 480 U.S. 340, 348–49 (1987)). Given the facts and circumstances, the Court cannot conclude that officers conducted the search in such a way that "minimize[d] unwarranted intrusions into an [Defendant]'s privacy." *Gregoire*, 2009 WL 5216844, at *8.

Though the Government does not argue the doctrine of inevitable discovery, this doctrine provides guidance regarding whether officers would have found the video simply because they had authority to search all data. In order for inevitable discovery to apply, the Government must show that: "(1) there was a reasonable probability that the evidence would have been discovered by lawful means in the absence of police misconduct, and (2) that the government was actively pursuing a substantial, alternative line of investigation at the time of the constitutional violation." *United States v. James*, 353 F.3d 606, 617 (8th Cir. 2003) (citation omitted).

Here, the warrant did give the authority to search Defendant's computer for the limited purpose of finding evidence of the failure to register as a sex offender and identity theft. However, as noted, OS Triage immediately began searching for items not related to travel or residency. If he had not used OS Triage, Deputy Walker could have either: gone through Defendant's computer files individually to look for evidence of the failure to register or identity

[3] It is concerning if law enforcement officers are, as Det. Roller and Deputy Walker testified, using OS Triage to search in cases not involving child pornography (such as fraud cases), particularly given the fact that program's standard settings will automatically search for known images of child pornography.

theft, or utilized a tool that was tailored to find such evidence. That is not what Deputy Walker did. Instead, he used a program he knew would search for images of child pornography despite the fact that the warrant did not permit him to do so. Perhaps if Deputy Walker had used a different approach for the search of the computer he or Det. Roller would have happened upon the sole video of child pornography, as other officers did in the cases on which the Government relies. But, given that there was only one video containing child pornography among the 480 videos and over 36,000 images located just by the OS Triage program, it cannot be said that that one video would have been found absent the overly broad search. Additionally, Defendant's expert testified that a search tailored to find evidence of travel and residency would likely not locate the video containing child pornography. As such, the Government has not met its burden to show the discovery of this video would have occurred by other means of searching.[4] *See Williams*, 690 F. Supp. 2d 829. Therefore, suppression of the video containing child pornography found on Defendant's computer on September 5, 2013 is warranted. Further, suppression of subsequent searches and seizures is appropriate as they are fruits of the poisonous tree. *McManaman*, 673 F.3d at 846.

III. Recommendation

Based on the foregoing discussion, it is hereby **RECOMMENDED** that Defendant's Motion to Suppress Evidence, (Doc. 76), be **GRANTED**, and that the video containing child pornography resulting from the search of Defendant's computer on September 5, 2013, and any evidence derived as a result of subsequent searches and seizures, be **SUPPRESSED**.

/s/ *David P. Rush*
DAVID P. RUSH
UNITED STATES MAGISTRATE JUDGE

DATE: October 12, 2016

[4] Moreover, no party disputes that the Government was not pursuing a substantial alternative line of investigation regarding Defendant's failure to register, identity theft, or possession or receipt of child pornography.